



# Apache Tomcat: AJP secret compared in non-constant time

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2026-43514
<b>State</b>	PUBLISHED
<b>Assigner</b>	apache
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-12 16:16:18 UTC
<b>Updated</b>	2026-05-12 18:17:27 UTC

**Description** Observable Timing Discrepancy vulnerability when comparing AJP secret in Apache Tomcat. This issue affects Apache Tomcat versions 11.0.0-M1 through 11.0.21, 10.1.0-M1 through 10.1.54, 9.0.0-M1 through 9.0.117, 8.5.0 through 8.5.100, 7.0.0 through 7.0.109, and 7.0.0 through 7.0.0.

## Risk And Classification

**Problem Types:** CWE-208 | CWE-208 CWE-208 Observable Timing Discrepancy

## Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Apache Software Foundation</a>	<a href="#">Apache Tomcat</a>	affected 11.0.0-M1 11.0.21 semver	Not specified
CNA	<a href="#">Apache Software Foundation</a>	<a href="#">Apache Tomcat</a>	affected 10.1.0-M1 10.1.54 semver	Not specified
CNA	<a href="#">Apache Software Foundation</a>	<a href="#">Apache Tomcat</a>	affected 9.0.0-M1 9.0.117 semver	Not specified
CNA	<a href="#">Apache Software Foundation</a>	<a href="#">Apache Tomcat</a>	affected 8.5.0 8.5.100 semver	Not specified
CNA	<a href="#">Apache Software Foundation</a>	<a href="#">Apache Tomcat</a>	affected 7.0.0 7.0.109 semver	Not specified
CNA	<a href="#">Apache Software Foundation</a>	<a href="#">Apache Tomcat</a>	unknown 7.0.0 semver	Not specified

## References

Reference	Source	Link	Tags
<a href="http://www.openwall.com/lists/oss-security/2026/05/12/10">www.openwall.com/lists/oss-security/2026/05/12/10</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="http://www.openwall.com">www.openwall.com</a>	
<a href="https://lists.apache.org/thread/2k654v5cq123npfsd1b2kk1y30owqb1m">lists.apache.org/thread/2k654v5cq123npfsd1b2kk1y30owqb1m</a>	security@apache.org	<a href="https://lists.apache.org">lists.apache.org</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)